O-RAN Perspective on Industrial Internet of Things: A SWOT Analysis

Talha Faizur Rahman, Minglong Zhang, Vuk Marojevic
Department of Electrical and Computer Engineering
Mississippi State University - MS
Email: {tfr42, mz354, vm602}@msstate.edu

***Abstract*—Internet of Things (IoT) is becoming increasingly popular due to its ability to connect machines and enable an ecosystem for new applications and use cases. One such use case is industrial IoT (IIoT) that refers to the application of IoT in industrial settings especially engaging instrumentation and control of sensors and machines with Cloud technologies. Industries are counting on the fifth generation (5G) of mobile communications to provide seamless, ubiquitous and flexible connectivity among machines, people and sensors. The open radio access network (O-RAN) architecture adds additional interfaces and RAN intelligent controllers that can be leveraged to meet the IIoT service requirements. In this paper, we examine the connectivity requirements for IIoT that are dominated by two industrial applications: control and monitoring. We present the strength, weakness, opportunity, and threat (SWOT) analysis of O-RAN for IIoT and provide a use case example which illustrates how O-RAN can support diverse and changing IIoT network services. We conclude that the flexibility of the O-RAN architecture, which supports the latest cellular network standards and services, provides a path forward for next generation IIoT network design, deployment, customization, and maintenance. It offers more control but still lacks products—hardware and software—that are exhaustively tested in production like environments.**

***Index Terms*—O-RAN, Industrial IoT, 5G and Beyond, Radio Access Network, AI.**

I. Introduction

The fifth generation (5G) of mobile communication is motivated by several factors, including high data rate communication, energy efficient communication, and ubiquitous connectivity. These factors categorize the 5G services into enhanced mobile broadband (eMBB), ultra-reliable and low latency communication (URLLC), and the envisioned massive machine type communication (MMTC). It is because of these services that 5G is being conceived for the Industrial Internet of Things (IIoT) where many industrial applications fall under URLLC category [1]. IIoT is proposed as part of the Fourth Industrial Revolution (Industry 4.0) as it is believed to reduce waste, optimize operations, and effectively monitor processes in small-medium enterprises (SMEs). Studies have shows that SMEs represent about 90% of the global businesses and more than 50% of the employment worldwide.

Often used interchangeably with the term Industry 4.0, IIoT is transforming the industry manufacturing business into modern digital organizations. The typical IIoT setting requires ubiquitous connectivity for systems, machines, and sensors for time critical monitoring and control. It is equally important to efficient utilize the machine/sensor resources to prolong network lifetime in IIoT environments [2]. Recently, researchers have put significant effort into defining the role of 5G in IIoT scenarios. In particular, private 5G networks are being designed and deployed for enterprise users to provide opportunities to optimize and refine business processes. Qualcomm released a white paper [3] in which they identify critical issues related to the deployment of private 5G networks in industrial environments to foster the operations of IIoT. Similarly, [1] presents an overview of conceptual and functional architectures of private 5G network for industrial use cases. There are design challenges associated with the deployment of private 5G networks for IIoT, such as the need for lightweight end-to-end network slicing solutions, control oriented radio resource allocation techniques, and seamless integration with time sensitive networking.

A detailed survey of 5G systems and the enabling technologies for IIoT is provided in [4]. Reference [5] proposes a 5G IIoT architecture and wireless services for advanced manufacturing scenarios and technologies. Similarly, the 5G services URLLC and eMBB are studied in the context of IIoT because 5G IIoT may achieve extremely high data rates, low latency with wide coverage, and relatively low power consumption [6].

Although 5G networks are being widely deployed and leveraged for many industrial verticals, in order to satisfy the various requirements from URLLC to ubiquitous connectivity, there are still many limitations of the 5G network supporting IIoT needs. For instance, the IoT network in construction industries usually requires very high quality of service (QoS) due to the concerns of worker's safety [7], [8], which implies that the network should be well optimized. In addition, considering scale, application, density and other features of different IIoT networks, flexible control and configuration, functional tailoring and automation are necessary. The two main next generation network principles—openness and intelligence—are indispensable for supporting such contexts. Unfortunately, today's cellular networks still use monolithic designs that have limited flexibility to support divers IIoT use cases. Such designs cause a series of limitations, including limited reconfigurability, limited coordination, and locked vendors for providing network components, slowing down innovation and diversification [9].

The Open RAN (O-RAN) Alliance [9] was formed in 2018

2023 IEEE International Conference on Industrial Technology (ICIT) | 979-8-3503-3650-4/23/$31.00 ©2023 IEEE | DOI: 10.1109/ICIT58465.2023.10143032

Authorized licensed use limited to: Malardalen University. Downloaded on October 28,2025 at 23:38:00 UTC from IEEE Xplore. Restrictions apply.

and introduces a new network architecture that offers solutions to these limitations. O-RAN promotes softwarization, virtualization, and artificial intelligence (AI)/ machine learning (ML) for RAN control. It increases the network flexibility, vendor diversity, and innovation through open interfaces. O-RAN splits functionalities of a 5G base station into a central unit (O-CU), a distributed unit (O-DU), and radio unit (O-RU) [1]. It also connects the units to intelligent controllers through open interfaces, which support control actions, messages, and policies between the RAN and the controllers.

IIoT is one of the focus areas of O-RAN. By facilitating the deployment of AI/ML solutions as part of the RAN intelligent controllers (RICs), it can provide better performance than legacy networks. O-RAN's architecture empowers the use of external information to optimize the network. The external information may include traffic periodicity and duration, provided by mobile edge computing (MEC) servers, application servers, or industrial control platforms. Based on such information and RAN specific information, the AI/ML models can generate strategies, decisions, or near-optimal settings for diverse situations to provide networking solutions independent from the equipment manufacturer.

This paper identifies the the requirements, expectations and major networking challenges of IIoT in Section II. Section III articulates the foundations, features and advantages of O-RAN. Section IV analyzes O-RAN for meeting the expectations of IIoT and performs an analysis of the strengths, weaknesses, opportunities, and threats (SWOT). Section VI provides the concluding remarks.

II. Requirements and Challenges in IIoT

IIoT is derived from IoT with aim to meet requirements in industrial settings. Regarded as an evolution of IoT, IIoT networks constitute of inexpensive nodes that are characterized by plug and play features, long lifetime, durability, etc. It is estimated that a smart factory would have connected IoT devices with a density of 0.5 per square meter [10]. For dense areas, the connection density increases to one connected device per square meter. The current design of IIoT enables integration and interconnection of isolated manufacturing plants/machines in order to offer efficient production and services with a long lifetime [11]. All these IoT devices must have a means of powering themselves either through batteries or energy harvesting. Energy harvesting is a promising solution for IoT devices to prolong their operation. However, this limits the device's capability for many applications that demand higher power. For this reason, finite power resources like batteries are needed to supply power but they require replacements, thus increasing the cost of operation and maintenance. Battery powered IoT devices in industrial settings typically use wireless technology and pose a challenge of minimizing the energy consumption while increasing their operational capability. To address this challenge, IIoT devices need to operate in modes that yields reduced power consumption. For this reason, the power saving mode (PSM) and extended discontinuous reception (eDRX) have been proposed for IoT operations [12]. PSM enables to wake up periodically, transmit data, monitor, process incoming messages, and go back to sleep. It is anticipated that a PSM-enabled IoT device that transmits once per day could operate for well over 10 years on two AA batteries. The eDRX mode is based on network initiated connectivity in which an IoT device wakes up periodically to check if there is any incoming data and, if not, it goes back to hibernation. This mode can achieve 4.7 years if the IoT device with two AA batteries transmits data once a day with a wake up period of 10 minutes [13].

Infrastructure-based machine-to-machine (M2M) networks are designed to meet stringent timing and reliability requirements. IIoT is driven by process automation with two important services, process monitoring and control applications, playing a significant role in this transformation. Process monitoring is related to sensory data for observing the status of industrial equipment. Process monitoring and supervision applications have relaxed packet loss and jitter requirements with a transmission delay on the order of seconds. On the other hand, control applications require exchanging information between controllers and machines (sensors and actuators) and, hence, pose much stricter transmission delay requirements, typically in milliseconds and with a transmission reliability of 99.9999% [1]. We summarized the requirements in Table I.

In industrial environments, wireless technologies are considered relevant for monitoring applications; however, for control applications studies are being conducted to employ alternative communication technology because control applications demand such stringent requirements. These control applications can be realized through wired technology; however, wireless technology offers more cost-effective and flexible solutions.

In order to fulfill the connectivity requirements, there are certain challenges that 5G needs to overcome. For instance, one of the critical challenges in 5G is guaranteeing the quality of service (QoS) of monitoring and control applications. However, the tightly-coupled parameters and network functionalities prevent from flexibly configuring and optimizing network resources to meet the expectations of such applications. It is, therefore, desired to have a software-based network slicing solution operating on physical network infrastructures to meet the diverse QoS requirements of IIoT applications. On the other hand, it is important to perceive that the performance indicators mentioned in Table I are spread over different network parts: physical layer (regarding data rate), RAN (regarding reliability) and core network (regarding latency). Industrial systems need to be scalable as advanced features/devices are added over time for continuous performance improvements. It is necessary for 5G networks to adapt in near real time to support industrial operations in changing environments/conditions.

III. O-RAN Architecture and Capabilities

The major technologies to construct open and programmable networks are software-defined networking (SDN)

[1] O-RAN's overall architecture and the functionalities of CU, RU and DU will be discussed in Section III.

Authorized licensed use limited to: Malardalen University. Downloaded on October 28,2025 at 23:38:00 UTC from IEEE Xplore. Restrictions apply.

TABLE I
IIoT CONNECTIVITY REQUIREMENTS [14].

Applications	Reliability	Latency	Data Rate
Monitoring	$\geq 99.9\%$	$\leq$100ms	0.1-0.5 Mb/s
Control	$\geq 99.9999\%$	$\leq$2ms	1-5 Mb/s

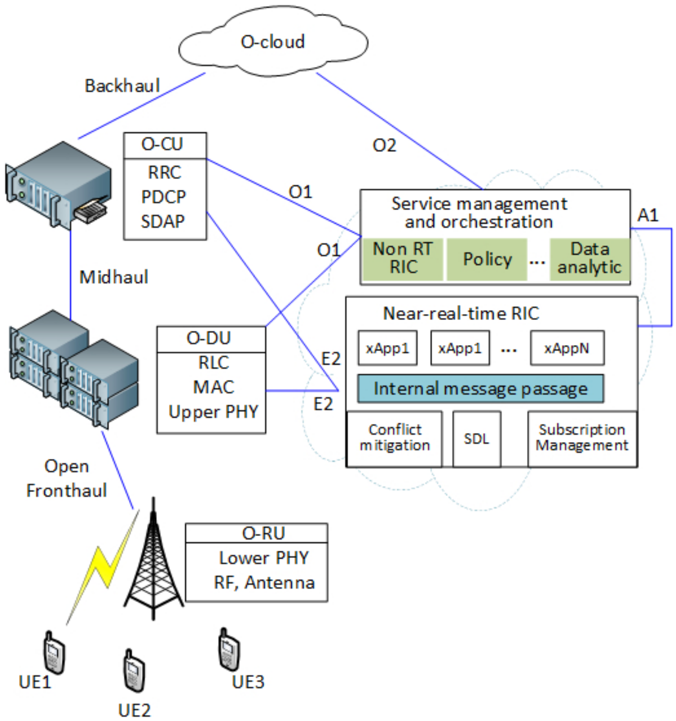

Fig. 1. O-RAN architecture, key components and interfaces.

and Cloud RAN (C-RAN). These have driven the transformation of wireless networks which have evolved to four fundamental O-RAN principles: disaggregation, intelligent control, virtualization, and openness.

A. Disaggregation

As shown in Fig. 1, the overall O-RAN architecture is defined in [15] and built upon the Third Generation Partnership Project (3GPP) RAN standard, adopting specific RAN functional splits, introducing new interfaces, two logical RICs, and the Service Management and Orchestration (SMO). More specifically, the O-RAN adopts split 2 for the higher-layer split (HLS) between the PDCP and RLC protocols, and split 7.2x for the lower-layer split (LLS), within the physical (PH)Y layer. Correspondingly, the RAN is disaggregated into the O-RAN Radio Unit (O-RU) at the cell site, the O-RAN Distributed Unit (O-DU) at Edge and the O-RAN Central Unit (O-CU) in regional servers or the Cloud. The O-RU mainly performs signal processing of the lower PHY layer, such as precoding, fast Fourier transform (FFT), cyclic prefix (CP) addition/removal. It is connected to the O-DU via the fronthaul. The O-DU is responsible for the upper PHY layer processing, Medium Access Control (MAC), and Radio Link Control (RLC). It connects to the Central Unit (O-CU) for higher protocol layer processing through the midhaul. The O-CU, on the other hand, implements a seriers of protocols at higher layers, mainly including the Radio Resource Control (RRC), the Packet Data Convergence Protocol (PDCP) and the Service Data Adaptation Protocol (SDAP) [9]. The operations in the disaggregated RAN units are tightly synchronized.

B. RAN Intelligent Controllers

The most remarkable feature of O-RAN is its RICs that enable programmable closed-loop RAN control and orchestration. The near-real time (RF) RIC and the non-RT RIC can both process key performance measurements of the network infrastructure and external context information. By applying AI/ML algorithms, the two RICs determine control polices and actions to optimize the network, enabling, among other, RAN slicing control, load balancing, and handover management. According to the O-RAN Alliance specifications, the non-RT RIC interacting with the network orchestrator operates on a time scale of beyond 1 second, whereas the near-RT RIC operates at a time scale between 10 milliseconds and 1 second.

The non-RT RIC is a component of the SMO framework. It communicates with the near-RT RIC to operate and control the RAN. Typically, it provides guidance, enrichment information and management of ML models for the near-RT RIC. It also affects operations in the SMO and indirectly governs all related components connected to the SMO, thereby adopting polices that are influential to thousands of devices attached to the RAN. In contrast, the near-RT RIC, which is deployed at the edge of the network, has direct connections with the CU and DU. As shown in Fig. 1, the near-RT consists of a number of customized applications, which are called xApps. Each xApp may have a specific functionality, from network status monitoring to radio resource management and allocation. In addition, data base storing the information otained from the RAN and an internal messaging infrastructure, the RIC Message Router (RMR), are also included in the near-RT RIC. It also provides services to handle security, manage subscriptions, resolve conflicts, and enable logging.

C. Virtualization

All the components of the O-RAN architecture can be virtualized on a hybrid cloud computing platform called O-Cloud [15]. The virtualization of O-RAN components is beneficial for cutting cost, facilitating deployment and portability. For instance, virtualization makes it possible to dynamically adjust the computing resources according to the network scale and user requirements, thus limiting the the power consumption to the actual network functions. RAN functions can be implemented as virtualized network functions [16]. The RIC cluster is developed on the Kubernetes platform and the xApps and rApps are thus deployed as containerized applications on Kubernetes [17]. The closed-loop controller in non-RT and near-RT RICs can fulfill dynamic sleep cycles for the base stations and the RF components.

D. Open Interfaces

The open interfaces specified by the O-RAN Alliance enable deploying different components of the RAN at selected

Authorized licensed use limited to: Malardalen University. Downloaded on October 28,2025 at 23:38:00 UTC from IEEE Xplore. Restrictions apply.

network locations, such as in the cloud, at the network edge, or at the cell site. As shown in Fig. 1, the near-RT RIC and the RAN nodes are connected via the E2 interface, which enables near-RT control loops and carries network performance and status information from the RAN and control instructions from the near-RT RIC. The near-RT RIC is connected to the non-RT RIC through the A1 interface, which enables non-RT control loops and data exchanges, providing the policy, guidance, and trained models to the near-RT RIC. The non-RT RIC can also directly connect to the RAN components for management and orchestration via the O1 interface. The non-RT RIC and the SMO also connect to the O-Cloud through the O2 interface. The interfaces between the O-RU and O-DU, between the O-DU and O-CU, and between the O-CU and the core network are standard open interfaces specified by 3GPP and O-RAN and are called open fronthaul, F1, and N2/N3, respectively [18].

IV. SWOT Analysis of O-RAN in IIoT

In this section, we provide a SWOT analysis of O-RAN technology for IIoT, summarized in Table II.

STRENGTH: Unlike in legacy networks where network functionalities are encapsulated and vendor-locked, the strength of O-RAN lies in enabling vendor agnostic functional decomposition of the RAN. Network slicing enables multiple tenants to share the physical infrastructure and provide multiple isolated services. IIoT networks are rather new and once deployed for supporting industry operations it is expected that network services will expand to further improve efficiency and adapt to changes in the production and manufacturing processes over time. O-RAN empowers the 5G network and enables IIoT networks to scale by defining open interfaces and disaggregating the software, which implements the network functionalities and controllers, from the hardware. It is worth noting that O-RAN provides a modular design, as shown in Fig. 1, in which the rApps in the non-RT RIC guide xApps in the near-RT RIC to achieve the desired performance gains. IIoT stakeholders (network or factory operators) can deploy customized xApps for managing the network and user devices as it grows. Software-defined network and control functions in O-RAN provide freedom and flexibility to stakeholders and facilitate manufacturing and network innovations on the fly without slowing down operations and business growth.

WEAKNESS: The near-RT RIC operates at a timescale of greater than 10 ms, whereas the non-RT RIC operates at a timescale of seconds or minutes. Industrial applications have diverse latency requirements. The primary weakness of O-RAN in its current form is its incapability to address latency requirements of control applications of less than 10 ms. RT Apps and a RT RIC is being sugggested by the academic community but it is not yet standardized. Because of the open interfaces, operators do not have to rely on specific vendors and are able to employ specialized solutions to react faster to changes in the service requirements. The potential risk of this is that the diversity of offered solutions from new providers and the ability to switch network components anytime may result in a lack of exhaustive testing and may pose security risks. While the interfaces are standardized and open, the internal functionality of network and control applications is implementation specific and may lead to vulnerabilities that may lead to network failures or attacks.

OPPORTUNITY: The openness of the O-RAN architecture and its interfaces allow to take advantages of a vendor-specific solutions for delicate applications or services. A massive number of devices in factories (e.g., meters, sensors, trackers) need to be connected to the network for smooth manufacturing operations. Although these devices may not generate huge amount of data, maintaining high densely deployed device is necessary. Dedicated xApps developed by third-party vendors, for instance, may add advanced features for sharing network resources. Digital twins are being deployed in various industries, such as the mining industry that typically requires both low latency, high data rates and high reliability for data transmission. An AI-based dApp deployed at O-DU can optimize physical-layer resource allocation to ensure these requirements can be satisfied. The xApp and the dApp can be developed by different providers with complementary expertise, which can potentially offer superior performance than a top-to-bottom solution provided by a single vendor.

THREAT: The dynamic disaggregation of functionalities and open interfaces also increase the risk of network security. The O-RAN Software Community (OSC) openly provides the software implementation of O-RAN functionalities which can be replicated, analyzed, exploited, and potentially modified by an adversary [18]. Intentional or unintentional software vulnerabilities can cause collapse of the network. Furthermore, the disaggregation of software and hardware, and improper ciphering of the data and control messages sent over open interfaces (ie., A1, E2, O1, O2) will make the network vulnerable. The xApps are the software applications that can be programmed to perform certain functions in the network, e.g., manipulating the behavior of a cell or performing intelligent radio resource management. A malfunctioning or malicious xApp may misconfigure network parameters or compromise network security to a level where serious damage can occur that may be difficult to localize and revert, which may considerably delay regular network operations and, in the case of IIoT, cause disruptions in the production processes and impact the business's reputation and competitiveness.

V. O-RAN Support for IIoT

As mentioned in Section II, IIoT services are characterized by their unique requirements in terms of latency, reliability and data rate. 5G systems are service-oriented with a wide variety of use-cases ranging from mobile broadband to reliable low latency communications. To satisfy the diverse QoS requirements, it is important to transform the conventional vendor-locked network architecture into a softwarized network architecture where the network element are deployable on general-purpose physical infrastructure. Such an architecture enables disruptive technologies, such as network slicing, network function virtualization, RICs, plug and play of new network

Authorized licensed use limited to: Malardalen University. Downloaded on October 28,2025 at 23:38:00 UTC from IEEE Xplore. Restrictions apply.

TABLE II
SWOT ANALYSIS OF O-RAN-ASSISTED IIoT.

Strength	Weakness	Opportunity	Threat
1. O-RAN enables sophisticated technologies, i.e., network slicing, suitable to meet diverse requirements of IIoT applications.	1. For real-time monitoring and control, sub-optimal AI/ML hyperparameter optimization in non-RT RIC may lead to poor near-RT RIC industrial O&M decision.	1. O-RAN enables third party developers to deploy customized xApps for IIoT usecases.	1. Due to programmable general-purpose hardware and the need for seamless coexistence of network functions and controllers, malfunctioning, malicious or incompatible softwaremay disrupt IIoT operations.
2. O-RAN enables scalability of IIoT network in manufacturing environments.	2. Due to lack of products, exhaustive testing and operations, the wide adoption of O-RAN in IIoT may take time.	2. The openness of O-RAN can help industries to work in collaboration with different IoT vendors	2. O-RAN increases the attack surface because of new interfaces, components, and third-party software and hardware solutions.
3. O-RAN allows stakeholders to deploy customized applications to control RAN operations.	3. O-RAN deployment requires new capital expenditures to upgrade or replace conventional IIoT network investments.	3. Real-time dApps will be game-changer in IIoT environments as sub-millisecond latency requirement can be met.	
4. O-RAN provides a platform to address data-driven IIoT environments through AI/ML controlling in SMO.			

elements, and dynamic network scaling. Network slicing is based on the principle of creating multiple logical networks across a common physical infrastructure where each of the logical networks is customized to meet specific application requirements and mapped to resources that are isolated from those of other slices. Industrial applications, as mentioned in Table I, demand strict isolation and performance guarantees, which can be achieved through customized slices with service level agreement (SLA). Certain IIoT control and monitoring services exhibit stringent latency requirements for which slice-specific resources can be provisioned. However, it has been shown that network slicing and scheduling is an NP hard integer programming problemfor which near-optimal solutions exist [4]. Recently, age of information (AoI) emerged as a new metric for industrial applications that quantifies the freshness of data and helps controllers to make timely decisions [19].

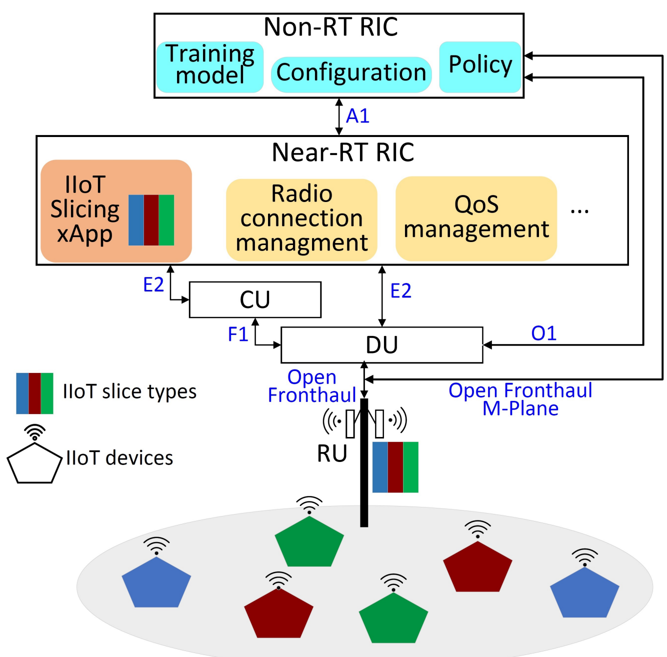

Fig. 2. Network slicing for O-RAN-assisted IIoT.

In order to accommodate different levels of QoS requirements regarding data rate, latency, reliability, and priority of IIoT applications, conventional RAN slicing which involves vendor-locked hardware and software does not provide sufficient flexibility and control. Reference [20] reveals how network slicing is supported in V-RAN and shows the effectiveness of real time control delegation and management of radio resources for providing performance guarantees of multiple coexisting services. Reference [21] proposes a deep reinforcement learning scheme to provide federated and dynamic network management and resource allocation for differentiated QoS services of future IIoT networks. In the proposed model, the deep Q-learning based slicing maximizes the QoS requirements in terms of throughput and delay, while the deep federated learning agents facilitate finding an optimal action decision. By balancing the cost of information updates from the IIoT devices with the device's energy consumption, the authors of [22] propose a two-sided distributed matching game in the O-RAN control layer that captures the IIoT channel characteristics and the IIoT service priorities to create IIoT device and small cell base station (SBS) preference lists. In addition, an actor-critic model with a deep deterministic policy gradient is employed to solve the resource allocation problem for optimizing the network slice configuration policy under time-varying slicing demands. Dynamic network slicing and AI-enhanced scheduling are the enabling technologies for future wireless network and service management. The loosely coupled network parameters and robust O-RAN architecture, enabling flexible network deployment, control, and scaling, are providing a framework for building reliable and extensible IIoT networks supporting a myriad of use cases.

Figure 2 shows the proposed modular design for network slicing in IIoT setting with O-RAN. The IIoT devices include sensors, controllers and other equipment in industrial environments. According to the different networking needs in terms of data rate, latency and reliability, among others, these devices can be divided into different groups. An IIoT slicing xApp in the near-RT RIC can process the resource needs of these groups to create custom slices for supporting data flows and the enabled services. Each slice may include a specific portion of network and radio resources. Moreover, xApps can dynamically control the RAN and, hence, the slices can be dynamically adjusted depending on resource utilization, utility

Authorized licensed use limited to: Malardalen University. Downloaded on October 28,2025 at 23:38:00 UTC from IEEE Xplore. Restrictions apply.

of the data, and other criteria to fulfill the service requirements. As the IIoT network increases or decreases the use of slices over time or as the industrial context evolves and changes priorities of data or process flows, the slicing xApp will receive new configuration and policy control information from the non-RT RIC which supports long-term network optimization. The xApp can then adjust the slices accordingly. The proposed solution based on O-RAN can effectively avoid redesigning the software and hardware framework when the IIoT network or the data/service priority changes.

VI. Conclusion

In this paper, we provide a perspective of IIoT supported by O-RAN. Unlike 4G mobile communication, 5G mobile communication is service-oriented that enables support for URLLC services that encompass most of the industrial connectivity requirements. However, 5G systems are closed systems that are encapsulated and do not allow much flexibility when it comes to hardware and software solutions from different vendors offering differentiated algorithms or services. It is for this reason that we recommend considering O-RAN which provides a flexible and open architecture with native support for RICs. Such architecture supports different IIoT settings and allows to customize the network parameters and controllers, enabling dynamic performance optimization, network scaling, supporting different connection densities and service priorities. We highlight the features of O-RAN and point out the advantages, challenges, opportunities and threats of O-RAN applied to IIoT. A major challenge of O-RAN is that software and hardware products are still limited and need to be exhaustively tested in production like environments. We are developing Open AI Cellular (OAIC) [23], a software platform that facilitates prototyping and testing of AI-enhanced RANs enabling 6G research. OAIC provides an open platform for the design, deployment and testing of xApps, rApps, and future real time Apps on software radio testbeds [24].

Acknowledgment

This work was supported in part by NSF award CNS-2120442.

References

[1] A. Aijaz, "Private 5G: The future of industrial wireless," *IEEE Industrial Electronics Magazine*, vol. 14, no. 4, pp. 136–145, 2020.

[2] T. F. Rahman, V. Pilloni, and L. Atzori, "Application task allocation in cognitive IoT: A reward-driven game theoretical approach," *IEEE Transactions on Wireless Communications*, vol. 18, no. 12, pp. 5571–5583, 2019.

[3] G. Brown and A. PRINCIPAL, "Private 5G mobile networks for industrial IoT," *Heavy Reading, White Paper, Qualcomm Inc*, 2019.

[4] A. Mahmood, L. Beltramelli, S. F. Abedin, S. Zeb, N. I. Mowla, S. A. Hassan, E. Sisinni, and M. Gidlund, "Industrial IoT in 5G-and-beyond networks: Vision, architecture, and design trends," *IEEE Transactions on Industrial Informatics*, vol. 18, no. 6, pp. 4122–4137, 2021.

[5] J. Cheng, W. Chen, F. Tao, and C.-L. Lin, "Industrial IoT in 5G environment towards smart manufacturing," *Journal of Industrial Information Integration*, vol. 10, pp. 10–19, 2018.

[6] B. S. Khan, S. Jangsher, A. Ahmed, and A. Al-Dweik, "URLLC and eMBB in 5G Industrial IoT: A survey," *IEEE Open Journal of the Communications Society*, vol. 3, pp. 1134–1163, 2022.

[7] M. Zhang, N. Ghodrati, M. Poshdar, B.-C. Seet, and S. Yongchareon, "A construction accident prevention system based on the internet of things (IoT)," *Safety Science*, vol. 159, p. 106012, 2023.

[8] M. Zhang, I. C. Lam, A. Kumar, K. K. Chow, and P. H. J. Chong, "Optical environmental sensing in wireless smart meter network," *AIMS Electronics and Electrical Engineering*, vol. 2, no. 3, pp. 103–116, 2018.

[9] M. Polese, L. Bonati, S. D'Oro, S. Basagni, and T. Melodia, "Understanding O-RAN: Architecture, interfaces, algorithms, security, and research challenges," 2022. [Online]. Available: https://arxiv.org/abs/2202.01032

[10] "Ericsson mobility report," Mar 2023. [Online]. Available: https://www.ericsson.com/en/reports-and-papers/mobility-report

[11] E. Sisinni, A. Saifullah, S. Han, U. Jennehag, and M. Gidlund, "Industrial internet of things: Challenges, opportunities, and directions," *IEEE transactions on industrial informatics*, vol. 14, no. 11, pp. 4724–4734, 2018.

[12] P. Lingala, S. Amuru, and K. Kuchi, "Experimental evaluation of power saving mode against powering down in an NB-IoT modem," in *2021 IEEE International Conference on Advanced Networks and Telecommunications Systems (ANTS)*. IEEE, 2021, pp. 325–330.

[13] "Designing cellular iot devices for battery life," Jun 2022. [Online]. Available: https://www.telit.com/resources/whitepapers/designing-cellular-iot-devices-for-battery-life/

[14] 3GPP, "Study on communication for automation in vertical domains," 3rd Generation Partnership Project (3GPP), Technical Report (TR) 22.804, 2017, v1.0.

[15] O-RAN Working Group 1, "O-RAN Architecture Description v6.0," ORAN.WG1.O-RAN-Architecture-Description-v6.0, O-RAN Standard, March 2022.

[16] M. Floriach-Pigem, G. Xercavins-Torregrosa, A. Gelonch-Bosch, and V. Marojevic, "Creating tailored and adaptive network services with the open orchestration C-RAN framework," in *2018 IEEE 5G World Forum (5GWF)*. IEEE, 2018, pp. 89–92.

[17] M. Kouchaki and V. Marojevic, "Actor-critic network for O-RAN resource allocation: xApp design, deployment, and analysis," in *2022 IEEE Globecom Workshops (GC Wkshps)*. IEEE, 2022, pp. 968–973.

[18] A. S. Abdalla, P. S. Upadhyaya, V. K. Shah, and V. Marojevic, "Toward next generation open radio access networks: What O-RAN can and cannot do!" *IEEE Network*, vol. 36, no. 6, pp. 206–213, 2022.

[19] H. H. Yang, C. Xu, X. Wang, D. Feng, and T. Q. Quek, "Understanding age of information in large-scale wireless networks," *IEEE Transactions on Wireless Communications*, vol. 20, no. 5, pp. 3196–3210, 2021.

[20] J. Thota and A. Aijaz, "Slicing-enabled private 4G/5G network for industrial wireless applications," in *Proceedings of the 26th Annual International Conference on Mobile Computing and Networking*, ser. MobiCom '20. New York, NY, USA: Association for Computing Machinery, 2020.

[21] S. Messaoud, A. Bradai, O. B. Ahmed, P. T. A. Quang, M. Atri, and M. S. Hossain, "Deep federated Q-Learning-Based network slicing for industrial IoT," *IEEE Transactions on Industrial Informatics*, vol. 17, no. 8, pp. 5572–5582, 2021.

[22] S. F. Abedin, A. Mahmood, N. H. Tran, Z. Han, and M. Gidlund, "Elastic O-RAN slicing for industrial monitoring and control: A distributed matching game and deep reinforcement learning approach," *IEEE Transactions on Vehicular Technology*, vol. 71, no. 10, pp. 10 808–10 822, 2022.

[23] OAIC:, "Open AI Cellular," https://www.openaicellular.org/, 2021, accessed: 2023-02-20.

[24] P. S. Upadhyaya, A. S. Abdalla, V. Marojevic, J. H. Reed, and V. K. Shah, "Prototyping next-generation O-RAN research testbeds with SDRs," *arXiv preprint arXiv:2205.13178*, 2022.

Authorized licensed use limited to: Malardalen University. Downloaded on October 28,2025 at 23:38:00 UTC from IEEE Xplore. Restrictions apply.